(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－195003

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
		３１０			３１０Ａ
	13/00	３５１		13/00	３５１Ｚ
// Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ
					６６０Ｄ

審査請求　未請求　請求項の数５　書面　（全８頁）

(21)出願番号　特願平9－370451

(22)出願日　平成９年(1997)12月27日

(71)出願人　598019462
窪田　悟
長野県長野市稲里町田牧417

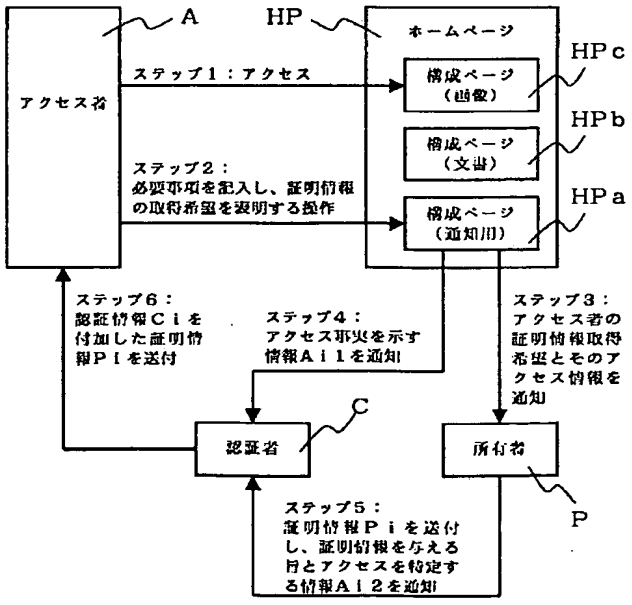
(72)発明者　窪田　悟
長野県長野市稲里町田牧417

(54)【発明の名称】　情報ファイルへのアクセスの認証方法

(57)【要約】

【課題】　ホームページにアクセスした事実を第三者の立場で確認し、ホームページ所有者がそのホームページにアクセスした者に与える情報に認証情報を付与することで、アクセス者が受け取る情報を正当なものとし、アクセス事実に反する情報が虚偽に作成されることを防止することを主目的とする。

【解決手段】　ホームページと呼ばれる情報ファイルＨＰにアクセスした事実を示す情報Ａｉ１を、アクセスを認証する認証者Ｃに知らしめる手段があり、情報ファイルＨＰの所有者Ｐは認証者Ｃ経由でアクセス者Ａに証明情報Ｐｉを与え、認証者Ｃは前記手段により知らされた情報Ａｉ１に基づき、アクセス者Ａに与えられる証明情報Ｐｉに当該アクセスの事実を認証する情報Ｃｉを付加することを特徴とする手段を講じる。



1

【特許請求の範囲】

【請求項１】　情報ネットワークによりアクセス可能に設定された情報ファイルと、前記情報ファイルへのアクセス者があって、前記情報ファイルの所有者もしくは管理者が、当該情報ファイルにアクセスした前記アクセス者に対し情報を与える場合において、前記情報ファイルにアクセスした事実を示す情報を、当該情報ファイルへのアクセスを認証する認証者に知らしめる手段があり、当該情報ファイルの所有者もしくは管理者は当該認証者経由で当該アクセス者に情報を与え、当該認証者は前記手段により知らされた情報に基づき、当該アクセス者に与えられる情報に、当該アクセスの事実を認証する情報、または当該アクセスを特定する情報及びその認証情報を付加することを特徴とする情報ファイルへのアクセスの認証方法。

【請求項２】　前記情報ファイルにアクセスした事実を示す情報を、当該情報ファイルへのアクセスを認証する認証者に知らしめる手段は、前記情報ファイルへのアクセス事実に基づく情報を当該認証者へ前記情報ネットワークを利用して通知する形態であって、当該通知情報の発信源を特定する情報が含まれ、または、当該通知情報の発信源から認証者が受信するまでの経路を特定する情報が含まれる情報の通知であることを特徴とする請求項１記載の情報ファイルへのアクセスの認証方法。

【請求項３】　前記情報ファイルへのアクセス者に与えられる情報が、画像情報を含む情報であることを特徴とする請求項１または２記載の情報ファイルへのアクセスの認証方法。

【請求項４】　前記情報ファイルへのアクセスの認証者が、前記アクセスの認証のために、前記アクセス者に与えられる情報に付加する情報は、当該認証者でない者が付加することができないか、もしくは当該認証者でないものが付加することが困難である情報であることを特徴とする、請求項１から３のいずれかに記載の情報ファイルへのアクセスの認証方法。

【請求項５】　前記アクセスの認証のために前記情報ファイルのアクセス者に与えられる情報に付加する情報は、電子透かしと呼ばれる技術に基づく情報であることを特徴とする請求項４に記載の情報ファイルへのアクセスの認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット上のホームページの所有者が、そのホームページへのアクセス者に対し、アクセスのお礼あるいは証明等のために画像等の情報を与える場合、その画像等の情報が、ホームページのアクセスの事実を示すものであることを第３者の立場で認証する手段に関する。

【０００２】

【従来の技術】アマチュア無線においては、交信が成立すると、交信者はお互いにＱＳＬカードと呼ばれる交信証を交換する。一方、ホームページと呼ばれる情報ファイルを、インターネットでアクセス可能とすることで、不特定者に提供している人がいる。ホームページの所有者が、自分の所有するホームページにアクセスした人に対し、アクセスのお礼やアクセス事実の証明のため、アマチュア無線のＱＳＬカードに相当する証明書を与える場合、従来の技術では、次のような手法をとることになる。

【０００３】一つは、図２に示すように、アマチュア無線同様、ホームページの所有者がアクセス者に対し、紙製のカードを与えることを基本とする。例えば、ホームページ上に、証明書の送付先を書き込むページを用意し、アクセスの証明書を希望する人は、そのページにアクセスして必要事項を書き込む。そして、送信アクションのボタンをクリックすると、書き込まれた情報がホームページの所有者に届くようになり、ホームページの所有者は、その情報に基づき、郵送等によりアクセス者に直接カードを送る、という手法がとられる。

【０００４】もう一つは、図２に示すように、ホームページの所有者がアクセス者に対し、電子メールにより文書等の情報を送ることを基本とする。例えば、ホームページ上に、証明書の送付先を書き込むページを用意し、アクセスの証明書を希望する人は、そのページにアクセスして必要事項を書き込む。必要事項としては、アクセス者の電子メールの受信アドレスが含まれる。そして、送信アクションのボタンをクリックすると、書き込まれた情報がホームページの所有者に届くようになり、ホームページの所有者は、その情報に基づき、証明やお礼の事項を記載した文書や必要に応じて画像等の情報を添付し、アクセス者に電子メールで送るという手法がとられる。

【０００５】

【発明が解決しようとする課題】このような従来の方法では、次のような問題点がある。まず、アクセス者の住所や電子メールのアドレスといった個人情報が、不特定の人に知られてしまうという問題である。第２に、従来技術によるところの電子メールで送られる情報は、誰でも同様の情報を作り出すことができるという問題である。単なるお礼としての情報であれば、虚偽の情報を作成しても特別の意味を持たないが、アクセス証明として扱われた場合、大きな問題となる。例えば、このようなアクセス証明情報を収集して、集まった証明情報がある条件を満たしたとき、その収集に対して何らかの賞を与えることが考えられるが、アクセス事実に反する虚偽の情報が作成されれば、虚偽情報により賞が与えられる恐れがある。従来の技術では、虚偽の情報作成を避けることはできなかった。

【０００６】本発明は、かかる問題点に鑑みてなされたものであり、ある者があるホームページにアクセスした

2

事実を第三者の立場で確認し、ホームページ所有者がそのホームページにアクセスした者に与える情報に認証情報を付加することで、アクセス者が受け取る情報を正当なものとし、アクセス事実に反する情報が虚偽に作成されることを防止することを主目的とする。また、ホームページの所有者からアクセス者にアクセスの証明等の情報を送る場合、アクセス者の住所や電子メールアドレスといった個人情報をホームページの所有者に明らかにする必要がなく、アクセス者が安心して不特定のホームページにアクセスし、その証明情報を取得できるようにすることを目的とする。

【０００７】

【課題を解決するための手段】上記の目的を達成すべく、本発明に関わる情報ファイルへのアクセスの認証方法は、情報ネットワークにより不特定者がアクセスできるように設定された一般にホームページと呼ばれる情報ファイルと、このホームページの所有者と、このホームページにアクセスするアクセス者と、このアクセス者のアクセス事実を認証する認証者との間で取り交わされる情報もしくは処理に関し、以下に示す手段をとる。

【０００８】請求項１記載の認証方法は、アクセス者がホームページにアクセスした事実を示す情報を、認証者に知らしめる手段を伴うことを特徴とする。この手段により認証者は、アクセス者がホームページにアクセスした事実を知ることができ、後述の認証を行うことが可能となる。

【０００９】アクセス者がホームページにアクセスした事実を示す情報を、認証者に知らしめる手段としては、例えば次のような処理を行う。ホームページにアクセス事実に関する事項を記載するページを備えておく。アクセス者はこのページにアクセスし、アクセス日時やアクセス者のＩＤ番号といったアクセス事実を示す事項を書き込む。アクセス事実を示す事項を書き込んだ後、アクセス者は、書き込んだ事項を送信するために設定されたホームページの表示画面に示された送信ボタンをクリックする。このクリックにより、書き込まれた事項は、インターネットに接続されているワークステーション等で実行されるプログラムに基づき、認証者にインターネットを通して送られる。同様にして、書き込まれた事項はホームページの所有者に送られるとよい。

【００１０】この際、アクセス者によって書き込まれた事項は、電子メールによって送られるようにプログラムされていてもよく、認証者が指定するデータベース等に書き込まれるようにプログラムされていてもよい。この書き込まれた事項を送る処理は、所有者側のワークステーション等が実行しても、アクセス者側のワークステーション等が実行しても、所有者側とアクセス者側の両方のワークステーション等が協調して実行してもよい。認証者に送られる情報は、アクセス者が書き込んだ事項に限定されず、例えばワークステーション等のプログラムの実行に関わる日時や処理番号等の情報を含めてもよい。また、アクセス者が送信ボタンをクリックする操作は必ずしも必要ではなく、ワークステーション等のプログラムにより、アクセスと同時に自動的にアクセスの事実を示す情報を認証者や所有者に知らしめるように構成してもよい。請求項１記載の認証方法は、このような手段に限定されるものではなく、アクセス者がホームページにアクセスした事実を示す情報を、認証者に知らしめる手段を備えていることを特徴とする。

【００１１】また、請求項１記載の認証方法では、ホームページの所有者がアクセス者にアクセスのお礼や証明等のために送る文書等の証明情報を、認証者経由でアクセス者に送ることを特徴とする。例えばこの証明情報を、アクセス者のアクセスより先に認証者に預けるような形態であらかじめ認証者に送っておくか、もしくはアクセス者のアクセス後に認証者に送り、認証者がアクセス者に送るという形態をとる。これにより、アクセス者の住所や電子メールアドレスといった個人情報は、認証者に知らせるのみで、ホームページの所有者には必ずしも知らせなくてよくなる。またこの手段により、ホームページの所有者からアクセス者へ与えられる証明情報に、認証者が認証情報を付加することを可能にする。

【００１２】請求項１記載の認証方法では、アクセスの事実を認証する情報やアクセスを特定する情報を含めた認証情報を、認証者がホームページの所有者から受け取った証明情報に付加することを特徴とする。アクセスの事実が認証者に知らしめられるのと同様に、ホームページの所有者もそのアクセスの事実と、アクセス者がそのアクセスに対する証明情報を要求していることを知らしめられている。そして、ホームページの所有者は、そのアクセス者に証明情報を送る場合は、アクセスを特定する情報を認証者に通知する手段をとる。アクセスを特定する情報とは、どのアクセス者のいつのアクセスに対するものか等を示す情報であり、アクセスの日時、ホームページの情報ファイル名、ホームページの所有者のＩＤ番号、およびアクセス者のＩＤ番号等が考えられる。次に認証者は、ホームページの所有者からのアクセスを特定する情報と、先に知らしめられたアクセスの事実を示す情報とを照合し、矛盾がない場合は、ホームページの所有者からの証明情報に認証情報やアクセスを特定する情報を付加し、その証明情報を認証する。そして、認証者は、認証情報等が付加された証明情報をアクセス者に送る。

【００１３】ホームページの所有者がこれらアクセスを特定する情報を認証者に伝える手段は、例えば、アクセス者に与えられる証明情報にそのアクセスを特定する情報を含め、その証明情報に示された情報をもって、認証者はアクセスを特定する情報を知る形態とするとよい。他にも、アクセスを特定する情報を、電子メールにより認証者に通知する形態としてもよい。証明情報を、あら

かじめ預ける形態として認証者に送る場合には、後者の手段をとる。

【００１４】認証者は、ホームページの所有者から送られた証明情報の対象となるアクセスと、知らしめられたアクセス事実に相違がないことを確認した後、アクセスを特定する情報と、その事実を認証する認証情報とを付加し、アクセス者に送る。アクセスを特定する情報は必ずしも付加する必要はない。例えば、ホームページ所有者の発行する証明情報にアクセスを特定する情報が示されていて、それが事実に反しない場合は、認証者が付加しなくても良い。また、アクセスを特定する情報の中に、アクセス事実を示す情報と厳密に一致しないものがあってもよい。例えばアクセス時刻は、許容範囲の中にあるときは、厳密に一致していなくとも正当なものとみなすことができる。

【００１５】請求項２記載の認証方法は、請求項１記載の認証方法において、ホームページへのアクセス事実を示す情報を認証者に知らしめる手段が、情報ネットワークを利用して通信する形態であることを特徴とし、その通信情報には、通信情報の発信源を特定する情報や発信源から認証者が受信するまでの経路を特定する情報が含まれることを特徴とする。情報ネットワークを利用することで、アクセス事実を直ちにしかも容易に認証者に知らしめることが可能となる。また、その通信情報に、通信情報の発信源を特定する情報が含まれるため、証明情報の受け取り者であるアクセス者自身がアクセス事実に反する虚偽の情報を認証者に知らしめることを防ぐことが可能となり、認証者が虚偽の情報に基づいて認証を行うことを防ぐことが可能となる。この通信情報の発信源は、ホームページがおかれたサーバーとなるようにすると、ホームページへのアクセスの事実と認証者へのアクセス事実の通信がより密接に対応し、認証者はより一層アクセス事実に対し忠実に認証を行うことが可能となる。

【００１６】請求項３記載の認証方法は、請求項１または２記載の認証方法において、ホームページの所有者からアクセス者に送られる証明情報が、画像情報を含むものであることを特徴とする。アクセスの証明情報がアマチュア無線のＱＳＬカードのような画像であれば、紙製のカードを発送することなく、紙製のカードと同じような感覚でアクセス者は証明情報を取得できる。さらに、その証明情報に本発明に係わる認証方法を適用することが可能となる。

【００１７】請求項４記載の認証方法は、請求項１から３に記載の認証方法において、ホームページの所有者がアクセス者に与える証明情報に付加される認証情報が、認証者でない者が付加することができないか、または認証者でないものが付加することが困難な情報とすることを特徴とする。これにより、認証情報を虚偽に付加することを防ぐことができ、アクセス者が受け取った情報が正当なものであるかどうかをより確実に判断できるようになる。また、アクセス者がホームページの所有者から認証者経由で受け取る証明情報を、虚偽に作成することをより一層困難なものにすることができる。

【００１８】請求項５記載の認証方法は、請求項４記載の認証方法において、ホームページの所有者がアクセス者に与える証明情報に付加される認証情報を、一般に電子透かしと呼ばれる技術に基づいて付加することを特徴とする。これによると、所有者からの情報が画像情報の場合であっても、画像を乱すことなく認証情報を付加することができるばかりでなく、認証者でない者が虚偽に作成することを極めて困難にすることができる。

【００１９】本明細書において、「ホームページ」とは、情報ネットワークによりアクセス可能に設定された情報ファイルの１つもしくはその情報ファイルの複数からなる情報ファイル群をさし、例えば、文書、画像、映像、音声、音楽、あるいはこれらの２以上の情報を含んだマルチメディア情報ファイルをさす。また、本明細書に記載するところのホームページの所有者は、ホームページの管理者等の所有者に準じる権利を有する者であってもよく、人に限定されるものではない。さらに、本明細書に記載するところの「認証者」とは、人に限定されず、法人、組織、機関、団体等を含んだ概念である。また、ホームページの所有者からアクセス者に与えられる情報を、本明細書では「証明情報」と記載しているが、何かを証明する情報に限定されるものではない。

【００２０】

【発明の実施の形態】以下、添付図面を参照して、本発明に係わる情報ファイルへのアクセスの認証方法を適用した実施の形態について説明する。

【００２１】図１は、本発明に係わる情報ファイルへのアクセスの認証方法を適用した場合の、認証手順を示す概念図である。インターネットによりアクセス可能に設定された情報ファイルとして、ホームページＨＰがある。アクセス者Ａは、インターネットを通じてこのホームページＨＰにアクセスし（ステップ１）、ホームページＨＰの文書や画像等の情報ＨＰｂ、ＨＰｃを見る。ホームページＨＰには、ホームページＨＰにアクセスしたことの証明情報Ｐｉをホームページ ＨＰの所有者Ｐが発行する旨の記載が、ホームページＨＰを構成するいずれかのページにある。アクセス者はこの記載を見て、証明情報Ｐｉが取得できることを知る。また、ホームページＨＰを構成するいずれかのページには、アクセス者がその証明情報Ｐｉの取得を希望していることを所有者Ｐに通知するための操作が施されるページＨＰａがある。この通知用ページＨＰａで導かれる操作をする（ステップ２）ことで、アクセス者Ａは所有者Ｐに証明情報Ｐｉを希望している旨を伝えられるように構成される。

【００２２】通知用ページＨＰａは、例えば、所有者Ｐが証明情報Ｐｉを発行するのに必要な事項を書き込むよ

うに設定され、アクセス者Ａは必要事項を書き込んだ後、画面上に示された送信ボタンをクリックするように導かれる。そして、必要事項を書き込み、送信ボタンをクリックすると、書き込んだ事項はホームページＨＰがおかれたサーバー（ワークステーション等）から所有者Ｐに通知される（ステップ３）。必要事項としては、例えば、アクセスの日時、アクセス者Ａの名前、アクセス者Ａに固有のＩＤ番号等が考えられが、必ずしもこれら全てを必要とするわけではない。ステップ３の通知は、インターネットを通じて所有者Ｐの指定するデータベースファイルに書き込まれるか、または、電子メールで送られることにより実施される。

【００２３】このような所有者Ｐへの通知機能は、必ずしもホームページＨＰがおかれたサーバから発信されなくてもよい。また、本明細書に記載するところの通知とは、その通知の受け取り者が確認できるように与えられるという概念をさし、通知の受け取り者がデータベース等にアクセスしてはじめてその内容がわかるように構成される場合を含んでいる。通知用ページＨＰａの動作や所有者Ｐへの通知機能は、ホームページＨＰもしくはＨＰａ、または、ホームページＨＰが置かれたサーバーや、アクセス者Ａのアクセスサーバーもしくはアクセス端末等の一つ、またはこれらの二つ以上によって処理される機能として実施される。また、通知用ページＨＰａは、他の画像や文章情報と共に、コンピュータディスプレイの同一画面内に表示されても構わない。ステップ３の通知は、後述の所有者Ｐから認証者Ｃへ通知されるアクセスを特定する情報Ａｉ２の基になる。

【００２４】アクセス者Ａが通知用ページＨＰａに導かれる操作を行うと、所有者Ｐへの通知と同様に、アクセス者Ａが通知用ページＨＰａに書き込んだ事項は、アクセスの事実を示す情報Ａｉ１として、認証者Ｃにも通知される（ステップ４）。ステップ４では、アクセス者Ａが書き込んだ事項のみでなく、通知の発信源となるサーバー（ワークステーション等）のＴＣＰ／ＩＰ通信プロトコルにおけるＩＰ番号、ドメイン名、処理日時、あるいは処理番号といった情報も含めて、認証者Ｃにインターネットを通して通知される。従って、認証者Ｃがステップ４におけるアクセスの事実を示す情報Ａｉ１を受信するまでに、この情報Ａｉ１がインターネット上のどのような経路を通ってきたかを認証者Ｃが知ることができるように設定することも可能となる。

【００２５】一方、所有者Ｐや認証者Ｃへの通知機能を、所有者Ｐと認証者Ｃに、アクセスの事実が矛盾なく正当に知らしめられなかったり、アクセスの事実に反する虚偽の情報を所有者Ｐと認証者Ｃに通知可能に実施した場合、アクセス者Ａの住所等の個人情報を所有者Ｃに知らせずに、アクセス者Ａは証明情報を得ることができるという本発明における最低限の目的は達せられることもある。しかしながら、この場合、本発明の効果の一部が無効となり好ましくない。

【００２６】ステップ３やステップ４は、通知用ページＨＰａにおけるアクセス者Ａの操作を必ずしも必要としない。例えば、ホームページＨＰが置かれたサーバーが、通信プロトコル上取得する情報に基づき、自動的に認証者Ｃや所有者Ｐに通知しても良い。さらに、所有者Ｐあての通知は、ホームページＨＰへのアクセスを通じて行うことに限定されない。例えば、電子メールや郵便等による文書で、ホームページへのアクセスとは別に、所有者Ｐに対しアクセスの証明情報を求める要求をすることにしてもよい。また、ステップ３とステップ４の順番は問わない。

【００２７】証明情報Ｐｉを希望する旨の通知を受けたホームページＨＰの所有者Ｐは、通知されたアクセス者Ａのアクセスに関する情報を参照する。そして、アクセス者Ａに証明情報Ｐｉを与える場合は、アクセス者Ａに対し証明情報Ｐｉを与える旨を認証者Ｃに通知し、証明情報Ｐｉを認証者Ｃに送る（ステップ５）。ここで、証明情報Ｐｉには、その証明情報Ｐｉの対象となるアクセス者ＡのホームページＨＰへのアクセスを特定する情報Ａｉ２を含める。アクセスを特定する情報Ａｉ２は、ステップ３により通知を受けた内容に基づくものである。

【００２８】この証明情報を与える旨の通知やアクセスを特定する情報Ａｉ２、および証明情報Ｐｉの送付は、一般に、電子メールやＦＴＰ（Ｆｉｌｅ　ＴｒａｎｓｆｅｒＰｒｏｔｏｃｏｌ）等のインターネットを利用した通信で行われる。証明情報Ｐｉは、アクセス者Ａのアクセスがあった後に認証者Ｃに送ってもよく、あらかじめ認証者Ｃに登録するような形態で与えておいてもよい。登録する形態とする場合は、証明情報Ｐｉを与える旨の通知と同様に、所有者Ｐはアクセスを特定する情報Ａｉ２を認証者Ｃに通知する。

【００２９】証明情報Ｐｉは、一般的には、発行者（通常ホームページＨＰの所有者）の意図で自由に定められるものであるが、受領者（通常アクセス者Ａ）の興味をそそるように、文章情報ばかりでなく、画像情報や音声情報が付加されるとよい。とくに、絵葉書のようなカードに相当する画像情報であると、受領者は視覚的に楽しめ、いろいろな人が発行する種々の証明情報を収集する興味が湧き好ましい。当然のことながら、証明情報Ｐｉは静止画像に限らず、ＧＩＦアニメーションであったり、動画情報であったり、画像として文字が記載されていたり、音声や音楽情報が付加されていてもよい。

【００３０】さらに、所有者Ｐに固有の情報を含めるとよい。例えば、所有者の意図により、所有者の居住する都市名や所有者固有のＩＤ番号の文字を画像中に表わす。これらの情報が示されていると、例えば、証明情報に記載された都市名が異なる証明情報を集め、日本全国の都市名を揃えるといったことが可能となり、このような証明情報を収集する興味が一層増すからである。所有

者固有のＩＤ番号は、例えば認証者Ｃといった公の機関から付与されることが望ましい。公の機関により特定されるＩＤ番号であると、同じ番号が付された異なる証明情報が発行されることが無くなるからである。同様にして、アクセス者にも固有のＩＤ番号が与えられることが望ましい。

【００３１】所有者Ｐがアクセス者Ａに証明情報Ｐｉを与える旨と、証明情報Ｐｉの対象となるアクセスを特定する情報Ａｉ２と、証明情報Ｐｉを受けた認証者Ｃは、アクセスの事実を示す情報Ａｉ１とアクセスを特定する情報Ａｉ２とを照合し、アクセス者Ａに証明情報Ｐｉが与えられることが正当であることを確認する。確認後、認証者Ｃは証明情報Ｐｉに認証情報Ｃｉを付加して、証明情報Ｐｉを認証する。認証情報Ｃｉの付加は、認証者Ｃが付加したことを特定でき、認証者Ｃでない者が虚偽に付加できないように行われる。そこで、一般に電子透かしと呼ばれる技術を用いることが好ましい。この方法によると、認証者Ｃは認証者Ｃ自身が付加した認証情報であることを特定でき、認証者Ｃでない者が虚偽に認証情報を付加することを防止できるばかりでなく、証明情報Ｐｉが画像情報であったとしても、その画像をほとんど劣化することなく認証情報を付加することができるからである。

【００３２】当然のことながら、アクセスを特定する情報Ａｉ２がアクセスの事実を示す情報Ａｉ１に合致しない場合は、認証者は認証情報Ｃｉを付加しない。また、ホームページＨＰが置かれたサーバーと何ら関わりのない発信源や経路によりアクセス事実を示す情報Ａｉ１が届いた場合、認証者Ｃはその通知を無効とみなし、認証を行わないようにすることも可能である。

【００３３】認証者Ｃは、認証情報Ｃｉが付加された証明情報Ｐｉを、電子メールやＦＴＰ等のインターネットを利用した通信によりアクセス者Ａに送る（ステップ６）。そして、アクセス者Ａは、ホームページＨＰへのアクセスに対する認証情報Ｃｉ付きの証明情報Ｐｉを取得することになる。

【００３４】最後に、認証情報Ｃｉが付加された証明情報Ｐｉの活用について、例を挙げて説明する。ここでいう証明情報は、アマチュア無線による交信を証明するＱＳＬカードに相当すると考えることができる。従って、第一に、ホームページの所有者が、自分のホームページをアクセスしてくれたお礼をアクセス者に伝えるという意味がある。第２に、アクセス者は、種々のホームページにアクセスし、様々な証明情報を収集することにある。製作者の個性が表れた証明情報を集めて楽しむわけである。さらに、証明情報に記載された情報に注目し、異なる情報が示された証明情報を集めて、ある一定の条件を満たすように証明情報を収集するのである。例えば、示された都市名が異なる証明情報を１００個集めるとか、日本全国の都市名を揃えるといったことが考えられる。証明情報に示された所有者のＩＤ番号に注目し、ＩＤ番号の最初の文字だけである単語が作れるように証明情報を集めることも考えられる。証明情報に示されたアクセス日に注目し、一年間に１００個の証明情報を集めるといった楽しみ方もある。このようなある特定の条件を満たすように、正当な認証情報が付加された証明情報が集められた場合、その収集に対し賞品や賞金を授与するといったことを行うと良い。

【００３５】また、ホームページの所有者相互に相手のホームページにアクセスし、証明情報を交換する場合、一方が証明情報を相手に与える旨を認証者に伝え、その相手の方も同様に証明情報を与える旨を認証者に伝え、証明情報を相手に与える旨の通知が交換する双方で揃ったときのみ、両者の証明情報を双方の相手に送るように認証者側で設定することもできる。さらに、たとえば１ヶ月以内といった期間を限定して、期間内に双方が相手のホームページにアクセスして、互いに証明情報を送る旨を認証者に通知しなければ、両者のアクセスが無効となり、いずれにも証明情報を送らないようにすることもできる。このように、認証者が認証した証明情報を送るための条件をつけるのは、容易に証明情報を取得できないようにするための手段である。授受の双方で人の操作が不要となると、コンピューター等により自動的に証明情報の取得を図るものが現れるかもしれない。そのような目論見を阻止する手段となりうるからである。

【００３６】

【発明の効果】以上のように請求項１記載の認証方法によれば、アクセス者の住所や電子メールのアドレスといった個人情報は認証者が把握していればよく、アクセス者の立場では、不特定のホームページにアクセスし、安心してその証明情報を得ることが可能となる。また、証明情報をアクセス者に与える際、認証者経由とすることで、認証者がアクセスの事実に基づく認証情報を付加することが可能となる。アクセス事実を示す情報は認証者に知らしめられているので、認証者はアクセス事実に忠実に認証を行うことができる。そして、その認証情報の有無により、アクセス者が受け取った情報が正当なものであるか否かが判断できるようになる。アクセス者が、ホームページの所有者が発行する証明情報を虚偽に作成したり、アクセスの事実に係わる証明情報の一部を改ざんするなどの不正な行為を行うことが困難になることは言うまでもない。

【００３７】さらに、請求項１記載の認証方法によると、認証情報の付加や証明情報の転送といったサービスに対し、認証者は、所有者やアクセス者から手数料を徴収することが可能であり、新たなビジネスを提供するという効果がある。本発明に係わる認証情報や証明情報の転送といったサービスがあって、そのサービス手数料を徴収することで認証者のサービスが充実し、アクセス者やホームページ所有者がより一層本発明に係わる認証方

法を利用しようとする効果も期待できる。また、様々な証明情報を収集し、一定の条件を満たすように認証情報が付加された証明情報を集めた者に対し、認証者は安心して賞品や賞金を授与することができる。したがって、アクセス者はこのような賞品や賞金を得るべく、より多くのホームページにアクセスし、より多くの認証を受けた証明情報を集めようとするので、認証者の手数料収入が一層増すという効果がある。

【００３８】賞品や賞金を授与するのは、認証者に限られたことではない。例えばホームページの所有者が企業であり、ホームページが企業の製品案内等を記載したものである場合、各製品ごとに異なる証明情報を用意し、一定の数の証明情報を取得した者に対し、ホームページの所有者である企業が賞品や賞金を授与することが考えられる。この場合、アクセス者としては、ホームページに示された情報を取得するのみならず、多くの証明情報と、場合によっては賞品や賞金を受けるという利点があり、ホームページの所有者である企業としては、より多くの製品案内を見てもらえるという宣伝効果が生じる。

【００３９】また、請求項２記載の認証方法によれば、情報ネットワークを利用してアクセスの事実を示す情報を認証者に通知するので、アクセス後直ちにその情報を認証者に知らせることができるばかりでなく、その情報の発信源や発信源から認証者が受信するまでの経路を特定することが容易になる。したがって、アクセスの事実を示す情報の発信源や経路が、アクセスされたホームページと無関係の場合は、認証情報を付加したり証明情報をアクセス者に送ったりしないようにできる。これにより、より一層不正を防止することができる。

【００４０】また、請求項３記載の認証方法によると、アクセスに対する証明情報を、アマチュア無線のＱＳＬカードのような画像情報により作成できる。ＱＳＬカードを集めるのと同様の感覚でホームページへのアクセスの証明情報を集めることができるようになる。さらに、紙製のカードとは異なり電子媒体であることから、証明情報を動画にしたり、音声や音楽を含めることも可能であるため、アクセス者は、ホームページの所有者の発行するオリジナリティある証明情報を収集する興味が一層増すという効果がある。

【００４１】また、請求項４記載の認証方法によると、認証情報を付加した認証者が特定できるばかりでなく、虚偽に付加することを防ぐことができる。従って、アクセス者が受け取った証明情報や、賞品や賞金を受けるべく提示された証明情報が正当なものであるかどうかをより確実に判断できるようになる。当然のことながら、賞品や賞金を受けようと、アクセスの事実に反する証明情報が虚偽に作成されることを防止できるという効果がある。

【００４２】さらに、請求項５記載の認証方法によると、認証情報が、電子透かしと呼ばれる技術に基づいて付加されるため、所有者からの情報が画像情報の場合であっても、画像をほとんど乱すことなく認証情報を付加することができる。そのうえ、認証者でない者が認証情報や認証情報付きの証明情報を虚偽に作成することを極めて困難にすることができるという著効がある。

【図面の簡単な説明】

【図１】本発明の実施の形態に係わる情報ファイルへのアクセスの認証手順を示す概念図である。

【図２】従来の技術に基づく、ホームページへのアクセスを証明する情報の発送手順を示す概念図である。

【符号の説明】

Ａ　ホームページへのアクセス者

Ａｉ１　アクセス事実を示す情報

Ａｉ２　アクセスを特定する情報

Ｃ　認証者

Ｃｉ　証明情報に付加される認証情報

ＨＰ　ホームページ

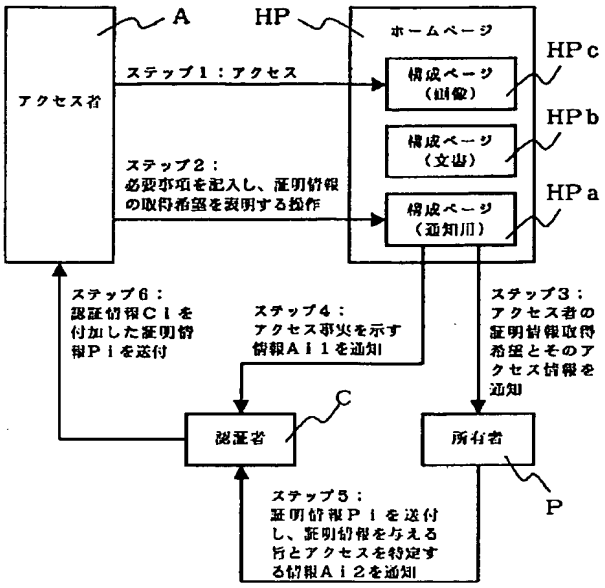
ＨＰａ　ホームページＨＰの構成ページである証明情報の希望通知用ページ

ＨＰｂ、ＨＰｃ　ホームページＨＰの構成ページ

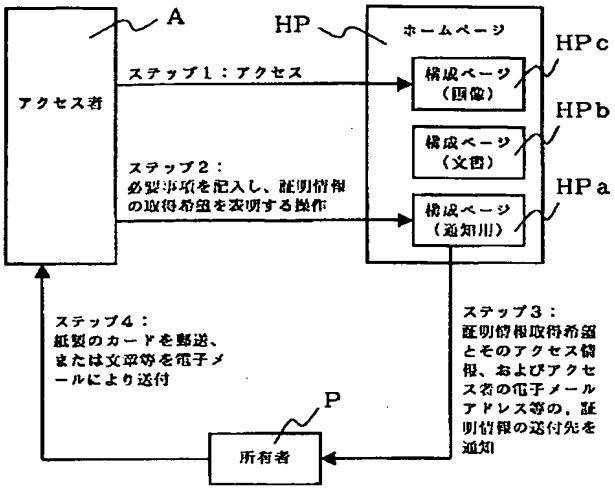
Ｐ　ホームページの所有者

Ｐｉ　アクセスを証明する証明情報

【図１】


A
HP
ホームページ
HPc
HPb
HPa
アクセス者
ステップ１：アクセス
構成ページ（画像）
構成ページ（文書）
構成ページ（通知用）
ステップ２：
必要事項を記入し、証明情報の取得希望を表明する操作
ステップ６：
認証情報Ｃｉを付加した証明情報Ｐｉを送付
ステップ４：
アクセス事実を示す情報Ａｉ１を通知
ステップ３：
アクセス者の証明情報取得希望とそのアクセス情報を通知
認証者
C
所有者
P
ステップ５：
証明情報Ｐｉを送付し、証明情報を与える旨とアクセスを特定する情報Ａｉ２を通知

【図２】


A
HP
ホームページ
HPc
HPb
HPa
アクセス者
ステップ１：アクセス
構成ページ（画像）
構成ページ（文書）
構成ページ（通知用）
ステップ２：
必要事項を記入し、証明情報の取得希望を表明する操作
ステップ４：
紙製のカードを郵送、または文章等を電子メールにより送付
ステップ３：
証明情報取得希望とそのアクセス情報、およびアクセス者の電子メールアドレス等の、証明情報の送付先を通知
P
所有者